Implementación de Servicios y Normativas clave de Ciberseguridad

Protección estratégica y cumplimiento normativo para el negocio real.

Raúl Gonzalo Martín

Analista de ciberseguridad

OBJETIVOS DE LA SESIÓN

Qué te llevas de esta sesión

1. El problema de negocio para PYMES
1. Principales normativas (RGPD, NIS2, ENS)
1. Medidas o herramienta de ciberseguridad
1. Servicios de ciberseguridad
1. Hoja de ruta práctica en 3 pasos para empezar

“Soy pequeño, a mí no me van a atacar”... la frase más peligrosa del sector.

El Mito de la Empresa Pequeña

"Soy pequeño, a mí no me van a atacar"... la frase más peligrosa del sector.

Objetivo

60% de los ataques son dirigidos a PYMES

Tipos de ataque

Ataques automatizados y no personalizados.

Impacto directo

- Facturación
- Reputación

Datos ciberataques

- + 26% en 2025
- Un total de 122.223

Ejemplos reales

Ransomware

Secuestro de datos. Archivos cifrados y actividad paralizada. Sin facturar, sin ERP, sin pedidos. **¿Cuánto tiempo puedes sobrevivir parado?**

Fraude del Correo

Suplantación de identidad para desviar pagos de facturas reales. El dinero vuela antes de que te des cuenta. **Pérdida financiera directa.**

Marco Normativo: RGPD, NIS2 y ENS

De la obligación legal a la exigencia del mercado.

RGPD

Protección de datos personales de clientes y empleados. Requiere medidas técnicas **demostrables**.

NIS2

Seguridad en la cadena de suministro. Tus clientes te pedirán **evidencias** para seguir siendo su proveedor.

ENS

Obligatorio para trabajar con la Administración Pública. Necesario para **licitaciones** y contratos públicos.

RGPD traducido a servicios

Medidas organizativas

- Política de protección de datos.
- Registro de tratamientos y proveedores.
- Plan de respuesta ante brechas.

Medidas técnicas

- Copias de seguridad y cifrado.
- Control de accesos y MFA.
- Monitorización básica de incidentes

RGPD traducido a daños

El Daño económico

20M€

O 4% DE FACTURACIÓN

Máxima multa legal por infracción muy grave (la AEPD aplica estas multas por fallos en los principios básicos).

El Daño Reputacional

- Las multas son graves, pero el mayor impacto en la empresa tras una brecha de datos es la pérdida de confianza. Los clientes no vuelven.

El peor castigo no es la multa, sino la vergüenza pública y la pérdida de negocio.

NIS2 y las PYMES

¿A quién aplica?

Aplica directamente a entidades “esenciales” e “importantes”

¿Afecta a las PYMES?

Muchas PYMES entran en su cadena de suministro

¿Que pide?

- Evidencias de gestión de riesgos
- Controles de seguridad y continuidad
- Gestión de incidentes y proveedores

ENS para proveedores

¿A quién aplica?

Afecta a AAPP y a muchos proveedores de servicios TIC

Distinción de niveles

Niveles (básico, medio, alto) según criticidad

¿Que exige?

- Análisis de riesgos
- Controles técnicos mínimos
- Procedimientos documentados

Apoyo

Puede servir también con apoyo para cumplir con NIS2.

Medidas / Herramientas

SEGURIDAD DE REDES Y EQUIPOS

FIREWALL GESTIONADO

Filtrado de tráfico y **perímetros** seguros configurados por expertos.

PROTECCIÓN ENDPOINT

Seguridad avanzada EDR para **proteger** cada dispositivo individual.

FILTRADO WEB

Bloqueo proactivo de sitios maliciosos antes de la infección.

ACTUALIZACIONES

Gestión **centralizada** de **parches** para eliminar vulnerabilidades.

COPIAS DE SEGURIDAD

Frecuencia (RPO)

Qué se copia y con qué periodicidad.
(RPO) Punto de recuperación

Nube / Offline

Garantizar que existe una copia aislada físicamente de la red principal.

Pruebas de Restauración

Validación periódica de que los backups son funcionales y recuperables.

COPIAS DE SEGURIDAD

El Estándar de Resiliencia:

- **3 Copias:** Mantener al menos tres copias de tus datos.
- **2 Soportes:** Almacenar copias en dos medios distintos (Disco/Nube).
- **1 Offsite:** Guardar una copia fuera de la oficina.

3-2-1

Fórmula de Supervivencia

GESTIÓN DE IDENTIDADES Y MFA

Los 4 pilares de la identidad

Autenticación

Uso de **MFA** en correo y aplicaciones de negocio críticas.

Higiene

Revisión periódica de usuarios y **cuentas** inactivas.

Privilegios

Asignación de **permisos** según el rol y mínimo privilegio.

Control

Reducción drástica de cuentas genéricas o compartidas.

GESTIÓN DE IDENTIDADES Y MFA

Doble factor de autenticación

Blindando el Acceso Externo

El MFA es la barrera más efectiva contra el robo de credenciales, especialmente en servicios expuestos a internet.

- Correo Electrónico: El principal vector de ataque.
- Apps Críticas: ERP, CRM y almacenamiento cloud.
- Facilidad: Apps de autenticación (MS Authenticator).

GESTIÓN DE IDENTIDADES Y MFA

Higiene

Limpieza de Usuarios Inactivos

Las cuentas de ex-empleados o cuentas de prueba olvidadas son puertas traseras ideales para los atacantes.

- **Eliminación:** Borrar usuarios que ya no pertenecen.
- **Revisión:** Auditoría trimestral de accesos.
- **Suspender:** Desactivar antes que eliminar para forensia.

GESTIÓN DE IDENTIDADES Y MFA

Privilegios

Zero Trust

"Nunca confiar, siempre verificar". La identidad es el nuevo perímetro de seguridad para la PYME.

PERSONAS Y CONCIENCIACIÓN

Formación y Concienciación

La mayoría de los ataques empiezan con un clic. Es vital:

- **Píldoras formativas:** Breves, prácticas y constantes.
- **Simulacros de Phishing:** Entrenar el ojo del empleado de forma segura.
- **Cultura de seguridad:** Que sepan qué hacer si sospechan de algo.

SERVICIOS BÁSICOS

PUNTO INICIAL: DIAGNÓSTICO

Diagnóstico inicial: “ITV”

Diagnóstico de Riesgos

Antes de disparar a ciegas, revisamos:

- Sistemas y datos críticos.
- Brechas de seguridad actuales.
- Plan de acción priorizado (Imprescindible vs. Recomendable).

Evaluaciones como servicio

Sellos o certificaciones

Diagnóstico del punto actual

Evaluación de la organización

- Cumplimiento de RGPD
- Madurez a nivel de ciberseguridad
- Gobernanza y gestión de la ciberseguridad
- Recomendación y asesoramiento

SERVICIOS AVANZADOS

SERVICIO AVANZADO 1:
Monitorización y gestión de vulnerabilidades

Análisis de Logs

Recogida y análisis exhaustivo de registros para identificar actividades sospechosas antes de que escalen.

Alertas Inteligentes

Notificaciones inmediatas ante comportamientos anómalos detectados en su red o equipos críticos.

Respuesta Activa

Ayuda especializada y soporte técnico directo en la contención y respuesta ante incidentes de seguridad.

SERVICIO AVANZADO 1:
Monitorización y gestión de vulnerabilidades

Seguridad Gestionada

Un Centro de Operaciones de Seguridad (SOC) actúa como la torre de control de su empresa, supervisando cada evento digital.

Nuestro equipo de expertos utiliza herramientas de vanguardia para garantizar que su negocio nunca se detenga debido a una amenaza externa.

SERVICIO AVANZADO 1:
Monitorización y gestión de vulnerabilidades

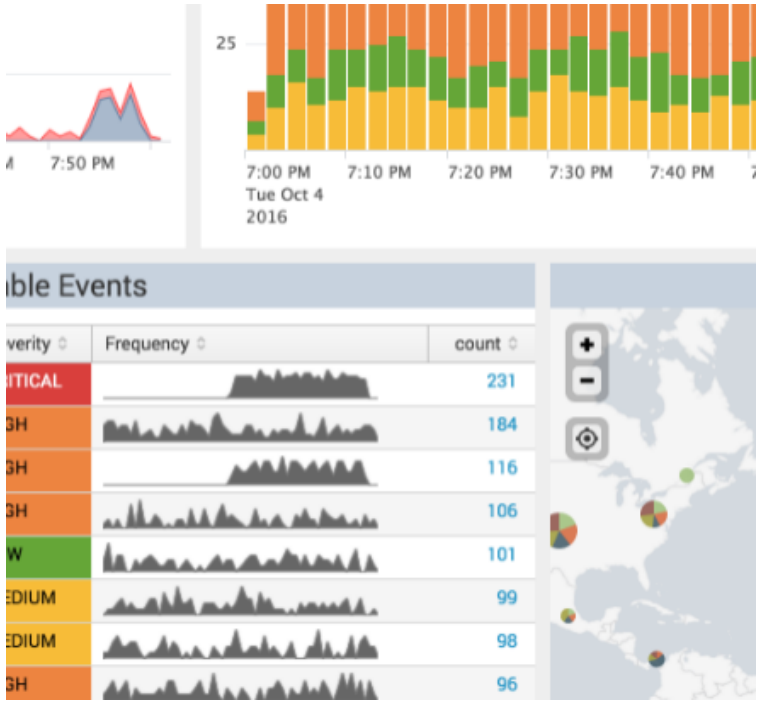
Característica	Monitorización Estándar	Servicio Avanzado SOC
Análisis de Logs	Reactivo (bajo demanda)	Proactivo (Tiempo Real)
Alertas de Anomalías	Umbrales fijos	Basadas en Comportamiento
Respuesta a Incidentes	Soporte Básico	Ayuda Directa Especializada
Gestión de Vulnerabilidades	Escaneo Anual	Monitorización Continua

SERVICIO AVANZADO 1:
Monitorización y gestión de vulnerabilidades

Identificar, Priorizar, Remediar

El ciclo de vida de la vulnerabilidad requiere una monitorización constante. No basta con saber que existe un riesgo; es vital saber cuál es su impacto potencial.

Nuestro servicio le ayuda a gestionar el ciclo completo, asegurando que los parches y actualizaciones críticas se apliquen en el momento justo.



SERVICIO AVANZADO 2:
Auditoría de ciberseguridad

Es un proceso **metodológico y legal** de evaluación exhaustiva y sistemática de la infraestructura tecnológica, políticas y prácticas de una organización para identificar **vulnerabilidades y riesgos.**

Objetivos:

- Prevenir incidentes (eficacia de controles)
- Cumplimiento normativo
- Confianza y reputación
- Mejora continua

"If you fail a penetration test you know you have a very bad problem indeed. If you pass a penetration test you do not know that you don't have a very bad problem" - Gary McGraw

SERVICIO AVANZADO 2:
Auditoría de ciberseguridad

Identificación Proactiva

No espere a ser atacado para conocer sus debilidades. El Pentesting simula ataques reales bajo condiciones controladas para:

- Detectar vulnerabilidades críticas.
- Evaluar la eficacia de sus defensas actuales.
- Garantizar lanzamientos seguros de aplicaciones.
- Cumplir con estándares de seguridad exigentes.

SERVICIO AVANZADO 2: Momentos críticos

Lanzamientos

Antes de poner en marcha nuevas plataformas o grandes cambios en la red.

Actualizaciones

Tras migraciones de sistemas o integraciones de terceros en su infraestructura.

Recurrencia

Revisiones periódicas para adaptarse a las nuevas amenazas del panorama actual.

HOJA DE RUTA: 3 PASOS

0-3 Meses

Diagnóstico inicial.

Tapado de brechas críticas.

MFA y Backup.

3-6 Meses

Políticas de seguridad.

Formación al personal.

Actualizaciones.

6-12 Meses

Cumplimiento ENS/NIS2.

Gestión vulnerabilidades.

Monitorización SOC.

SEGURIDAD COMO VENTAJA

No se trata solo de evitar multas.

La ciberseguridad es hoy una condición necesaria para ser un proveedor confiable.

Si no puedes demostrar que tus procesos son seguros, tus clientes buscarán a alguien que sí pueda.

Gracias por su atención